



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

[Signature]

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/356,600	07/19/1999	WILLIAM DUANE	SDT-040	8046

21323 7590 12/02/2004

TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER

ARANI, TAGHIT

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/356,600	DUANE ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani, Ph.D.	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 April 2004.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,3-5,10,11,13,14,17,18 and 52-90 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,3-5,10,11,13,14,17,18 and 52-90 is/are rejected.
- 7) Claim(s) 55,60 and 76 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-51 were originally pending for examination.

Claims 2, 6-9, 12, 15-16, 19-51 are now canceled.

Claims 52-90 are newly added.

Claims 1, 3-5, 10-11, 13-14, 17-18, 52-90 are pending.

Applicant's amendment filed on April 4, 2004 necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL, see MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Objections

Claims 55, 60 and 76 are objected to because of the following informalities: "identifyies" in claim 55 should be "identifies". "cryptrographic" in claims 60 and 70 should be "cryptographic". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 54-69, 3-4, 10, 70-90 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Claims 54 and 70 contains the subject matter " encrypted container" which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Dependent claims 55-69, 3-4, 10 and 71-90 are also rejected by virtue of their dependencies.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 54 recites the limitation "the identified encrypted container" in line 8. There is insufficient antecedent basis for this limitation in the claim.

Dependent claims 55-69, 3-4 and 10 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 11, 52 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record Holloway, U.S. Pat. No. 6,424,718 and further in view of Linehan et al. (hereinafter "Linehan), U.S. Patent 5, 495, 533 issued Feb. 1996.

As per claims 1, Holloway teaches a method for securely providing information comprising the steps of:

(a) at a storage sever, receiving from the client information identifying an encrypted personal security device [col. 7, lines 48-53, i.e. when a user claiming to be authorized accesses a WWW page on the web server via a browser on a client. The server compiles the applet Ap which includes the claimed users encrypted private key (i.e. encrypted personal security device) stored on the key server, and all of the associated cryptographic algorithms].

(b) in response to receiving- said information identifying a personal security device,
sending from the storage server to the client providing said identified encrypted personal
security device [in a preferred embodiment, Holloway discloses that a private key (i.e. a
personal security device) of a user is stored in a storage portion of a key server or written to a
data storage means to which the server has access. The private key is delivered from server
system to a user within an applet Ap via web server and World Wide Web (WWW), see col.
7, lines 30-67];

Holloway teaches at the browser, the private key is decrypted if the claimed user knows the owning pass phrase (PPu) which establishes the identity of the owning user (i.e. if the user is authenticated). Holloway fails to teach:

(c) at an authentication server, receiving authentication information from the client;

and

(d) responsive to said authentication information, sending from a key server to the
client

decryption information for said personal security device.

However, Linehan teaches :

(c) at an authentication server, receiving authentication information from the client

[See abstract , see Fig. 4, Authentication server 34, col. 7, lines 54-64]; and

(d) responsive to said authentication information, sending from a key server to the
client

decryption information for said personal security device [Fig. 4, personal key server 32 sends the file encryption key to the client , wherein the key decrypts the data as it is read from the file].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Holloway to include the personal key server and authentication server of Linehan to authenticate the user, then provide the decryption key to decrypt the Holloway's applet Ap at the user's browser, because disadvantages of manual key management (such as entering Holloway's owner's pass phrase PPu) include the awkward and time-consuming requirements for end-users to enter encryption keys, the possibility that users may forget keys, the inability to access encrypted files when the individual who knows the keys is unavailable [Linehan, col. 2, lines 12-24].

As per claim 11, Holloway teaches a method implemented by a client for accessing secure information comprising the steps of:

(a) receiving from a storage serve an encrypted personal security device [col. 7, lines 48-53, i.e. when a user claiming to be authorized accesses a WWW page on the web server via a browser on a client. The server compiles the applet Ap which includes the claimed users encrypted private key (i.e. encrypted personal security device) stored on the key server, and all of the associated cryptographic algorithms];

Holloway teaches at the browser, the private key is decrypted if the claimed user knows the owning pass phrase (PPu) which establishes the identity of the owning user (i.e. if the user is authenticated). Holloway fails to teach:

(b) receiving from a key server decryption information for said personal security device; and

(c) decrypting said personal security device.

However, Linehan teaches:

(b) receiving from a key server decryption information for said personal security device [Fig. 4, personal key server 32, see also col. 7, lines 62-64, see also col. 9, lines 55-56]; and

(c) decrypting said personal security device[col. 7, lines 63-64, see also col. 9, lines 57-58].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Holloway to include the personal key server of Linehan to provide the decryption key to decrypt the Holloway's applet Ap at the user's browser, because disadvantages of manual key management (such as entering Holloway's owner's pass phrase PPu) include the awkward and time-consuming requirements for end-users to enter encryption keys, the possibility that users may forget keys, the inability to access encrypted files when the individual who knows the keys is unavailable [Linehan, col. 2, lines 12-24].

applet Ap is correct an the user is authentic, see col. 9, lines 10-38].

10. (Currently Amended) The method of claim 54, wherein the received authentication information includes a time-based authentication code.

As per claim 52, Holloway teaches the method of claim 1, further comprising implementing the storage server and the authentication server on the same computer [col. 8, lines 40-44].

As per claim 53, Holloway teaches the method of claim 1, further comprising implementing the authentication server and the key server on the same computer [col. 8, lines 40-44].

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
AUG 21 2006